

INFORMIEREN. AGIEREN. VORBEUGEN.



[IT in der Wolke >](#)

[< Silver Tipps für Silver Surfer](#)

Falsche Freunde im Internet

Soziale Netzwerke werden immer öfter für kriminelle Zwecke missbraucht



Büroklatsch hat in sozialen Netzwerken nichts verloren

©creativcollection Verlag GmbH

Soziale Netzwerke wie [Facebook](#), [Twitter](#) oder [Xing](#) bieten faszinierende neue Möglichkeiten der Kommunikation. Doch sind auch hier bereits Kriminelle aktiv, die Daten klauen, Nutzer abzocken oder belästigen. Wir bieten einen Überblick über die wichtigsten Risiken und eine Reihe praktischer Sicherheitstipps.

Achtung Gefahr!

Kriminelle haben sich auf die besonderen Umgangsformen in sozialen Netzwerken bereits gut eingestellt und nutzen die Funktionen von [Facebook](#) und Co., um Nutzer zu schädigen. Hier ein Überblick der wichtigsten Gefahren:

- ▶ Betrüger schleusen über soziale Netzwerke schädliche Computerprogramme ein, etwa durch das Posten von Links, die auf manipulierte Webseiten führen.
- ▶ Datenfischer locken Nutzer durch gefälschte Nachrichten auf täuschend echt nachgebaute Seiten und fordern sie dort zur Eingabe von Zugangsdaten auf. Mit Hilfe der ergaunerten Daten können sie dann Nachrichten verschicken, in denen sie beispielsweise finanzielle Notsituationen vortäuschen und von Freunden des Opfers Geld erbitten.
- ▶ Private Informationen in sozialen Netzwerken werden von möglichen Arbeitgebern als Entscheidungsgrundlage genutzt oder von Betrügern in fremde Webseiten integriert.
- ▶ Skrupellose Werber sammeln Adressdaten oder persönliche Informationen von Nutzern, um diesen ungefragt Werbung anzuzeigen oder zu schicken.
- ▶ Cybermobber können im Schutz der elektronischen Anonymität Personen viel leichter bloßstellen oder bedrängen als in der „echten Welt“. Dabei hilft ihnen die Flut an Informationen, die sie über die sozialen Netzwerke über ihre Opfer beziehen können.
- ▶ Ein Nutzer will private oder berufliche Informationen, die er in einem sozialen Netzwerk platziert hat, löschen – er hat aber keinen Einfluss mehr darauf, da sie sich bereits im Netz verbreitet haben.



Nicht nur echte Freunde lesen mit

©creativcollection Verlag GmbH

Einfache Maßnahmen - große Wirkung!










Wer sich vor den Gefahren in sozialen Netzwerken schützen möchte, muss nicht gleich ganz auf deren Nutzung verzichten. Hier eine Reihe von Tipps, wie Sie sich sicherer durch Ihre Online-Community bewegen können:

- ▶ Geben Sie nicht zu viel über sich preis! Und überprüfen Sie Ihre Datenschutzeinstellungen, so dass nicht jeder Besucher Ihres Profils alle Informationen zu sehen bekommt.
- ▶ Akzeptieren Sie nur solche Personen als Kontakte, die sie auch wirklich kennen – „falsche Freunde“ wissen sonst etwa sehr schnell, wann Ihre Wohnung leer steht, und können diese Informationen auf kriminelle Weise nutzen.
- ▶ Achten Sie auf den Einsatz sicherer Passwörter. Nach Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) sollten diese mindestens acht Zeichen lang sein und neben Buchstaben auch Ziffern und Sonderzeichen enthalten. Außerdem sollten Sie für verschiedene Anwendungen auch unterschiedliche Passwörter nutzen.
- ▶ Seien Sie vorsichtig mit dem Nachverfolgen von Links! In sozialen Netzwerken werden immer öfter von Datenfischern manipulierte Links platziert, um Nutzer auf gefälschte Seiten zu

Das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** bietet auf seiner **Webseite** ausführliche Informationen über die Risiken der sozialen Netzwerke und Möglichkeiten, sich dagegen zu wehren.

- ▶ locken, um so an die Zugangsdaten zu kommen. Damit kann die Identität des Nutzers gestohlen und für kriminelle Zwecke missbraucht werden.
- ▶ Vorsicht beim Download von Inhalten aus dem Internet in soziale Netzwerke – Sie könnten dadurch Urheberrechte verletzen und sich strafbar machen.
- ▶ Achten Sie darauf, dass Ihr Computer durch ein Virenschutzprogramm und eine Firewall gesichert ist und aktualisieren Sie dieses Programm regelmäßig.

Folgende Artikel könnten Sie auch interessieren:

-  [Ursachen und Formen von Cybermobbing](#)
-  [Sehen und gesehen werden](#)
-  [Für wen gilt das Jugendstrafrecht?](#)
-  [Legales Verhalten üben](#)
-  [Brandschutzprävention im Kindergarten](#)
-  [Prävention von Cybermobbing im Schulkontext](#)
-  [Verherrlichung von Magersucht und Suizid im Netz](#)
-  [Gier und Neugier](#)
-  [Zehn Tipps zu Ihrer Sicherheit im Internet](#)

[Alle Artikel dieser Kategorie](#)

Weitere Infos zum Thema Internet und Mobil



Hoaxes und Kettenbriefe erkennen

Falschmeldungen im Internet

Sie erhalten eine Mail von einem Kollegen, in der eine Stiftung...[\[mehr erfahren\]](#)



Vorsicht bei billigen Angeboten

Fake-Shops bei Amazon

Immer wieder fallen Käufer auf so genannte „Fake-Shops“ bei Amazon...[\[mehr erfahren\]](#)



Gefahren und Datenschutz

Wer will an meine Daten?

Wir hinterlassen Datenspuren, jeden Tag, auf verschiedene Weise: Im...[\[mehr erfahren\]](#)



Falschmeldungen im Internet

Fakt oder Fake?

„Papst unterstützt Donald Trump“, „Obama ist ein Muslim“, „Angela...[\[mehr erfahren\]](#)



Online-Portal informiert Ältere rund um Internetsicherheit und Datenschutz

Silver Tipps für Silver Surfer

Ob E-Mail, [Phishing](#), Smartphone oder Online-Shopping – vielen...[\[mehr erfahren\]](#)

© Verlag Deutsche Polizeiliteratur

Cookie Einstellungen

- Statistiken
- Essentiell

Wir nutzen Cookies auf unserer Website. Einige von ihnen sind essenziell, während andere uns helfen, diese Website und Ihre Erfahrung zu verbessern.

Nur essentielle Cookies akzeptieren Alle akzeptieren